Ecole Normale Supérieure Paris Année 2013-2014
Algèbre 1

Corrigé de la Feuille d'exercices 3

Exercice 4.

a) Soient G_0 l'ensemble des générateurs de G et g_0 un élément de G_0. Alors si φ est un automorphisme de G, l'image de φ est engendrée par $\varphi(g_0)$; ce qui veut dire que $\varphi(g_0)$ est un générateur de G. On définit alors une application (ensembliste) $\begin{array}{ccc} \mathrm{Aut}\, G & \to & G_0 \\ \varphi & \mapsto & \varphi(g_0) \end{array}$. Comme g_0 est générateur, l'application est bijective.

b) Dans $\mathbb{Z}$, montrons par récurrence sur $k \geq 0$ qu'il existe a_k premier avec p vérifiant $(1+p)^{p^k} = 1 + a_k p^{k+1}$. L'étape d'initiation est triviale. Si l'on suppose $(1+p)^{p^k} = 1 + a_k p^{k+1}$, on obtient $1 + p^{p^{k+1}} = 1 + p^{k+2}(a_k + \sum_{i=2}^{p} C_p^i a_k^i p^{(i-1)(k+1)-1})$ et le résultat est montré par récurrence. En particulier, $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
Montrons maintenant que tout sous-groupe fini H du groupe multiplicatif d'un corps k est cyclique. En effet, pour $d|n$, notons μ_d le nombre d'éléments d'ordre d dans H. Supposons $\mu_d > 0$ et soit y un élément d'ordre d. Alors, parce que k est un corps, le sous-groupe engendré par y est formé des éléments de H qui satisfont $x^d = 1$. On déduit que $\mu_d \leq \varphi(d)$. Le théorème de Lagrange nous assure l'égalité $n = \sum_{d|n} \mu_n$. D'autre part, en regardant les ordres des éléments dans $\mathbb{Z}/n\mathbb{Z}$, on sait que l'on a $n = \sum_{d|n} \varphi(d)$. Au final, on a donc $\mu_d = \varphi(d)$ pour tout $d|n$; en particulier, on a $\mu_n = \varphi(n) \geq 1$, et H est bien cyclique.
En appliquant ce fait à $\mathbb{F}_p$, on voit que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, d'ordre $p-1$. Notons x_0 un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et prenons un relèvement x_1 de x_0 dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. L'élément x_1 est d'ordre $(p-1)p^s$ pour un certain $s \leq \alpha$, de sorte que $x := x_1^{p^s}$ est d'ordre $p-1$. Comme x et $1+p$ ont des ordres premiers entre eux, les sous-groupes qu'ils engendrent ont intersection réduite à l'élément neutre. Et comme le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, on a $(x(1+p))^k = x^k(1+p)^k$ et cette puissance vaut 1 si et seulement si $x^k = 1$ et $(1+p)^k = 1$. On en déduit que k est divisible par $p^{\alpha-1}$ et par $(p-1)$, donc par $p^{\alpha-1}(p-1)$ (puisqu'ils sont premiers entre eux). L'élément $x(1+p)$ est donc d'ordre $p^{\alpha-1}(p-1)$ et $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

c) Remarquons d'abord $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Supposons maintenant $\alpha \geq 2$. Par une récurrence semblable à celle effectuée au (b), on montre que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Observons maintenant le morphisme $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$. Son noyau contient H le sous-groupe engendré par 5 et, par cardinalité,

on a en fait une égalité. Si on note $K = \{\pm 1\}$, on a que $KH = (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ et $K \cap H = \{1\}$. On déduit que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq K \times H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

d) Si $\prod_p p^{\alpha_p}$ est la décomposition en facteurs premiers de n, alors le lemme chinois nous donne

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/2^{\alpha_2}\mathbb{Z})^\times \times \prod_{p\neq 2,\, \alpha_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha-1}\mathbb{Z}\big).$$

Exercice 5. En remarquant qu'un groupe cyclique ne peut pas contenir plus d'un élément d'ordre 2, on conclut que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2^\beta p^\alpha$ avec p un nombre premier impair, $\alpha \geq 0$ et $\beta \in \{0, 1\}$ ou $\alpha = 0$ et $\beta = 2$.

Exercice 6. Soient $p_1, \ldots, p_n$ des nombres premiers distincts. Considérons le sous-groupe additif de $\mathbb{R}$ engendré par $\log(p_1), \ldots, \log(p_n)$. Si $a_1, \ldots, a_n \in \mathbb{Z}$ sont tels que $a_1 \log(p_1) + \cdots + a_n \log(p_n) = 0$, alors en prenant l'exponentielle on trouve $p_1^{a_1} \ldots p_n^{a_n} = 1$ donc $a_1 = \cdots = a_n = 0$.
Vous pouvez aussi prouver que le groupe engendré par $2^{(2^{-i})}$, $1 \leq i \leq n$ convient aussi.

Exercice 7. On peut voir G en tant que sous-groupe de $\mathbb{Q}^n$. Soit $e_1, \ldots, e_r$ un système libre maximal de $G = \mathbb{Z}^n$.

1. Supposons $r > n$. Alors $e_1, \ldots, e_r$ n'est pas libre sur $\mathbb{Q}$ donc il existe $q_1, \ldots, q_r \in \mathbb{Q}$ tels que $q_1 e_1 + \cdots + q_r e_r = 0$. En multipliant par le ppcm des dénominateurs des $q_1, \ldots, q_r$ on peut supposer que $q_1, \ldots, q_r \in \mathbb{Z}$. Donc $e_1, \ldots, e_r$ n'est pas libre.

2. Supposons $r < n$. Alors $e_1, \ldots, e_r$ n'est pas une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$, donc il existe e_{r+1} qui n'appartient pas au $\mathbb{Q}$-sous-espace vectoriel engendré par $e_1, \ldots, e_r$. Donc $e_1, \ldots, e_r, e_{r+1}$ est libre sur $\mathbb{Z}$ et $e_1, \ldots, e_r$ n'est pas maximal.

Exercice 8. L'exercice équivaut à trouver une matrice dans $\mathrm{GL}_n(\mathbb{Z})$ dont la première ligne est formée des entiers $a_1, \ldots, a_n$. On le montre par récurrence sur n. Soit d le pgcd de $a_1, \ldots, a_{n-1}$ et notons $a_i' = a_i/d$ pour tout $1 \leq i \leq n-1$. Alors, par hypothèse de récurrence, il existe un matrice $(n-1) \times (n-2)$ D tel que la matrice

$$\left(\begin{array}{ccc} a_1' & \ldots & a_{n-1}' \\ \hline & & \\ & D & \\ & & \end{array}\right)$$

appartienne à $\mathrm{GL}_{n-1}(\mathbb{Z})$. Par hypothèse $\mathrm{pgcd}(a_n, d) = 1$ donc il existe $v, w \in \mathbb{Z}$ tels que

$a_n v + dw = 1$. Alors la matrice

$$\left(\begin{array}{ccc|c} da'_1 & \dots & da'_{n-1} & a_n \\ \hline & & & 0 \\ & & & 0 \\ & D & & 0 \\ & & & \vdots \\ & & & 0 \\ -va'_1 & \dots & -va'_{n-1} & w \end{array}\right)$$

convient.

Exercice 9. On montre d'abord l'exercice dans le cas où G est libre ou fini. Ensuite on utilise la décomposition $G = L \oplus F$ où L est la partie libre de G et F la partie finie. Il est aussi facile de montrer que $\mathrm{Hom}(F, L) = 0$.
Soit $\{e_i\}$ une base de L. Alors pour tout $f \in F$, l'élément $(e_i, f) \in L \oplus F$ s'envoie vers un certain (e'_i, f'_i), où $\{e'_i\}$ est une base de L et $f_i \in F$ (car $\mathrm{Hom}(F, L) = 0$ et on connait le résultat quand $F = 0$). On déduit que la préimage d'un élément de la forme $(0, f')$ doit être de la forme $(0, f)$. Donc la restriction de notre morphisme du départ à F est une surjection vers F, donc un isomorphisme. Le noyau de notre morphisme vaut donc 0 et il est donc injectif.

Exercice 10.

a) On peut supposer $n \geq 4$, tout automorphisme de $\mathscr{S}_i$ pour $i \leq 3$ étant intérieur. Le groupe symétrique $\mathscr{S}_n$ est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geq 2$. Parce que τ_i et τ_j ne commutent pas si $i \neq j$, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont un point de support commun, qu'on notera α_1. Comme $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$, il ne peut en être autrement: tous ont α_1 en commun. On écrit alors $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. On a ensuite $\{\alpha_1, \dots, \alpha_n\} = \{1, \dots, n\}$ par injectivité de φ. Reste à définir la permutation $\alpha \in \mathscr{S}_n$ par $\alpha(i) = \alpha_i$ pour tout i: φ est la conjugaison par α.

b) Décomposons σ en produit de cycles à supports disjoints, k_1 cycles d'ordre 1, ..., k_n cycles d'ordre n, avec $n = \sum_i i k_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ, et donc envoyer un k-cycle sur un k-cycle (éventuellement trivial). Aussi, le commutant d'un n-cycle de $\mathscr{S}_n$ est composé des puissances de ce dernier. En mettant ceci bout à bout, on prouve que l'on a

$$|\mathrm{comm}\, \sigma| = \prod_i k_i! i^{k_i}.$$

c) Soit φ un automorphisme de $\mathscr{S}_n$. Si τ est une transposition de $\mathscr{S}_n$, $\varphi(\tau)$ est aussi d'ordre 2 et est un produit de k transpositions. Aussi, on a $|\mathrm{comm}\, \tau| = |\mathrm{comm}\, \varphi(\tau)|$, ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Comme on a $n \neq 6$, ceci impose $k = 1$. Par la question (b), φ est alors intérieur.

d) Supposons l'existence de H d'indice n dans $\mathscr{S}_n$ non conjugué à $\mathscr{S}_{n-1}$ (vu comme sous-groupe fixant $\{1\}$). On a un morphisme

$$\varphi : \mathscr{S}_n \to \mathscr{S}(\mathscr{S}_n/H) \simeq \mathscr{S}_n$$

provenant de l'action de $\mathscr{S}_n$ sur $\mathscr{S}_n/H$ par translation à gauche. Le noyau de φ est contenu ne peut être que $\{1\}$, $\mathscr{A}_n$ ou $\mathscr{S}_n$ par simplicité de $\mathscr{A}_n$. Mais il est contenu dans H et est donc trivial. Par cardinalité, φ est un isomorphisme qui envoie $\mathscr{S}_{n-1}$ sur H. De ce fait, φ n'est pas intérieur.

e) Le groupe $\mathrm{PGL}_2(\mathbb{F}_5)$, vu comme sous-groupe de $\mathscr{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$, n'est pas conjugué à $\mathscr{S}_5$ puisqu'il ne fixe aucun point. Le groupe $\mathscr{S}_6$ possède donc au moins un automorphisme extérieur.